Unleashing the power of innovative aerospace technology....

Roundups

Air Force
Research Laboratory
AFRL

news@afrl

Spring 2000

Official voice of the Air Force Research Laboratory

Lab moves, identifies messages using ancient tactic

by Fran Crumb, Information Directorate

ROME, N.Y. — Engineers at the Air Force Research Laboratory Information Directorate are working with researchers from a small computer security firm in the New York southern tier to address a high-tech threat with origins dating back more than three millennia.

"Steganography Detection and Recovery Toolkit," is the title of a six-month, $119,400 contract awarded to Wetstone Technologies Inc. of Freeville.

"The word 'steganography' is derived from Greek and means 'covered writing.' It is a military communications tactic that has been around since ancient times," said John C. Faust, program manager in the directorate's Defensive Information Warfare Branch. "During the era of the Roman Empire, military commanders would shave a messenger's head, write a message on the sheared scalp and — once the hair grew back — send the messenger through enemy lines.

"The concern in the computer age is that you can actually embed messages, data or code in images," Faust said. "If a computer picture has 256 different colors, just a minute change in color is not perceptible to the human eye. A person could embed a hidden message, a challenge to computer security or even classified information in a picture of their dog or cat — or a very innocuous photo from their family vacation."

Free software is currently available on the Internet that allows computer users to implement steganography technology for covert communications within a photograph. The goal is security through obscurity as opposed to encryption, where someone intercepting the communication is aware that data is being sent but it is not decipherable.

Ironically, scientists and engineers in the directorate's Information and Intelligence Exploitation Division have several on-going projects to develop such technology for military communications using digital watermarking embedded within photographs.

For those in the defensive information warfare field, however, the goal is to unmask this hidden data — which could carry a computer virus or mask critical information changes in a system without the user's knowledge. **@**